SECURITY REQUIREMENTS AND APPLICATION SCENARIOS FOR NATIONAL IDENTIFICATION CARD SCHEMES

Teddy Hsu
Information Security Group,
Royal Holloway, University of London
Surrey TW20 0EX, UK
C.HSU@rhul.ac.uk, Tel: +441784 466531

June 12, 2003

Abstract

Applications of a national ID card scheme have been discussed extensively worldwide. However, despite their fundamental importance, security issues for such a scheme have not been widely discussed. This paper considers detailed security and operational requirements for National ID card schemes, and the appropriateness of a variety of different card technologies to meet these requirements. This is achieved by examining in detail three application scenarios for such cards. The paper concludes with conclusions regarding the best technologies for such IC card application.

Keyword: ID Card Scheme, Application Scenarios, ID Card Security Requirements, Levels of Security, Card Technology, Evaluation.

1 Introduction

In today's digitised world people need improved means to identify themselves to other parties while requesting services or gaining entry to premises. With rapidly growing interests in deploying secure national identification card schemes in many parts of the world, it is important to define the possible applications of a national identification card scheme. Unless the scope of application of such cards is examined carefully and the security requirements identified, as is the intention of this paper, there is a danger that major potential advantages of such cards will be missed.

This paper is structured as follows. In section two of this paper, security requirements for a national ID card scheme are discussed. This is followed in section three by a review of the various possible card technologies that can be applied in such a scheme. In section four we define levels of security for an ID card scheme according to the types of threats and the impacts from those threats. In section five, the main part of this paper, three scenarios for use of such a national ID card in a variety of applications are developed, and in each case the types of data used, the identification check procedures and any potential problems are considered. These scenarios are then used to identify and authenticate a set of requirements for each application of the identification card scheme. A list of issues to be addressed before an appropriate technology can be chosen is also provided.

2 General Requirements for a National ID Card Scheme

The underlying function of a national ID card scheme is to identify the cardholder to a computer system or a government officer. Although user identification and authentication are the principal functions, many other functions could also be incorporated into the same scheme. Incorporating multiple functionalities into one means of providing identification would potentially be valuable to both citizens and other organisations such as banks and post offices.

Any ID card must meet certain basic operational and security requirements, which we now list. These requirements can conveniently be subdivided into User Identification requirements, i.e. those relating directly to the function of identifying the cardholder, and General requirements. We consider these two classes of requirements separately.

2.1 User Identification Requirements

The ID card must provide the ability to accurately identify and authenticate the cardholder. We can further sub-divide this into three separate requirements:

- The card must be able to provide information regarding the identity of the cardholder, including the cardholder name and potentially one or more numbers by which the cardholder is known to the relevant systems. For example, a passport has both the holder's name and the passport number.
- Means must be provided on, or in, the card to enable the card user to authenticate the cardholder. That is, the card must enable third parties to verify that the individual presenting the card is the individual who has the identity indicated on the card. For example, in some countries passports indicate certain distinctive features of an individual such as eye colour or height.
- The card must incorporate means to prevent forgery of, or modification to, cards. For example, holograms can be embedded in the card surface (as widely used in credit cards today), or special inks can be used.

2.2 General Requirements

The following more general requirements for an ID card scheme can also be identified.

- Depending on what types of hardware are involved in the ID card, communications between the ID card, card reader, remote terminal, and back end server must be secure.
- The overall design of the ID card scheme must address the integrity, confidentiality, and privacy of data being transmitted and processed.
- Personal information stored on ID card and at any centralised database server must be held securely, and only authorised personnel must be permitted to access such information.
- All communications channels in the ID card system must be secure.
- The ID card system must possess the ability to address personal privacy concerns.

In a closed environment (e.g. a company-wide ID scheme) it is easier to implement an online system in which the application of the ID card can be supported by a central system. Protocols can be designed for use company-wide and also with their trading partners. However, once a large number of interoperating organisations are involved, some general agreement about how to manage such an application is required, e.g. via standardisation — currently such a broad agreement over the operation of ID card system is lacking. It is also likely that, in an open environment, the identification procedure will need to involve at least two levels of identification and authentication. This will mean the card must be able to authenticate the cardholder (e.g. by matching a PIN or biometric data) as well as the issuing organisation (e.g. by checking a certificate and exchanging cryptographic keys).

3 Identification Card Technologies

There are a number of available card technologies that might be used as the basis of a personal identification scheme. We now review the main candidate technologies for ID cards and briefly consider their respective advantages and disadvantages.

Plastic Cards: such cards typically contain printed cardholder identification and authentication information such as name, photo, address, date of birth, etc. Such cards are used in applications where information can be visually verified when the card is presented by the cardholder. Such cards are not machine-readable and are very prone to forgery.

Bar Code Cards: with these cards data is represented as bar codes written on the card during the printing process. A bar code can store personal information, and, depending on the type of bar codes used, different amount of information can be stored. E.g. linear bar codes can be used to store a modest amount of simple alphanumeric data, whereas two-dimensional bar codes can store much more information in a small amount of space. Bar code cards can be scanned and the information obtained can then be displayed on a terminal. Such cards are machine-readable but the bar code can easily be copied.

Magnetic Stripe Cards: Cards of this type have been widely used for many types of application since 1970s. Information is written to the magnetic stripe during the personalisation process. They can be inserted into, or swiped through, readers at the point of interaction, and relevant information read from the card. To help prevent forgery, such cards can also contain forms of visual security features, such as those used on plastic cards, for example the embedding of laser holograms

in the card.

Optical Stripe Cards: this type of card uses a similar technology to that employed by write-once CDs, namely Write Once Read Many (WORM) technology. Such technology allows data to be read and added but not deleted or erased. The high storage capacity of such technology (up to multiple megabytes) allows such cards to be used in a wide range of applications. Examples of possible application domains include health care, identification, and other applications that require storage of a large amount of data.

Smart Cards [2]: are plastic cards that include an embedded chip. A smart card can be either a microprocessor card with internal memory and processing power or just a memory chip card[1]. Interactions between a reader and the card itself can be performed either via physical contact or by means of a remote contactless electromagnetic interface. All such cards have the ability to store much more data than bar code or magnetic cards, and microprocessor-based cards also have the ability to carry out on-card functions (e.g. cryptographic functions and key pair generation). Because microprocessor-based smart cards can perform calculations involving secret information without revealing this information to any external devices, such cards offer a range of security features not supported by other card types.

4 Levels of Security

The level of security required from an ID card depends on the types of threat and the possible impacts of these threats. The threats and their impacts will clearly depend on the type of application in which the card scheme is being used. When designing the application it is also necessary to decide on the level of tolerance of falsified or stolen cards, i.e. what is the maximum allowable probability that a false card will be accepted . The level of fault tolerance will depend on what information is being held in the database and what information is released after checking procedure. We must also consider the role of the identification card in the whole system and what responsibility the identification procedure holds. This means we need to decide whether the card is the only form of defence against attackers or only forms part of the whole defence system. After that we need to consider what the possible outcomes are and, same as the requirements, those

[1]The memory chip card is the simplest type of smart card, and in some sense such cards are not 'smart' at all. They contain memory circuits that are directly accessible through contacts using predefined protocols.

should be quantified too.

Things we need to consider include: what objects would be affected by a particular type of threat; what are the causes and how it would affect the system operation; what are the possible costs of such threat; how long would it take to bring a failed system caused by a threat back to normal; to name just a few. Next we will look at each possible type of ID card application and identity the requirements for the following issues: Type of Data and their Sensitivity; Identification Check Process; Privacy and Security Requirements. We tend to categorise the level of data sensitivity as Highly Confidential, Average Confidential, and Low Confidential. Highly Confidential data should only be revealed to the legitimate cardholder and/or authorised government agents. Average Confidential data can be revealed and/or referenced by request from other government authorities other than those pre-approved. Data categorised as Low confidential can be revealed and referenced without formal request/authorisation.

5 Application Scenarios for ID Cards

Individuals are required to confirm their identities for many purposes — from verifying identity and eligibility within a health care system, to accessing a secure network and services [1]. In this section we examine three examples of possible application of a national identification card scheme. We also discuss the types of data used, possible scenarios for use of the ID card, ID check procedures, and related requirements. Although the discussions are specific to the applications considered, it is hoped that the chosen application domains are sufficiently representative that the discussions will also capture requirements associated with most other likely application.

5.1 Travel Document

5.1.1 Type of Data and Sensitivity

If the card scheme is designed to be used as a travel document[2] (or part of the scheme's applications), it will usually require the following data to be available

[2]Here a travel document is means of providing and authenticating an individual's ID when travelling either domestically or internationally. It can be used either alongside or as a replacement for existing ID documents such as a passport or existing national ID card

when carrying out routine checks against one's identification: Name, Sex, Legal Nationality, Permanent Address, Employment Status, Criminal Activity Records, Resident Status, VISA Records. In terms of data sensitivity, we can categorise them as follows: Highly Classified - Criminal Records; Average Confidential - Employment Status, VISA Records; Low Confidential - Name, Sex, Legal Nationality, Permanent Address, Resident Status.
In this ID application the principal objective is for an officer (a manned terminal) to be able to identify an individual therefore granting permission to entry or denial of entry. To do this the officer needs to have access to (at least) the following information: Name, Legal Nationality, Resident Status, and VISA records. The highly confidential criminal records can only be revealed when the system returns an alarming result on identification check.

5.1.2 ID check Procedures

To carry out a routine check against an individual's identification, an airport/custom officer needs to perform the following procedures:

1. Physical Identification of cardholder.
2. The ID card is then inserted into the card reader or scanned.
3. At this point the remote terminal will access its own database server to retrieve necessary information to identify such individual and this could mean performing checks against name, sex, nationality, and VISA.
4. Card is returned to the cardholder and entry/depart granted.
5. If the check returns an alarming result (e.g. cardholder's name matches criminal names stored in the database), the officer needs to perform further actions.
6. Request would be made to be able to cross-reference with external databases and data sent to relevant authorities.
7. The notified authority would carry out further checks and makes final decision on adequate actions.

5.1.3 System Requirements and General Problems: Data Storage, Security and Privacy

In each step the system relies heavily on the verification process and the freshness of data to ensure the check's accuracy. In such system we would also require high

efficiency to ensure free flow of travellers due to the nature of a busy premise such as an airport. Also the system relies heavily on the task of verifying information to ensure accuracy and consistency. Every step is also related to each other and we would also require that the system be functioning properly to provide a good level of service. One of the problems we can see here starts when cross-referencing is required. There is a great level of privacy issue involved here because checking one particular database would easily result in further cross-referencing with other databases. This requires careful planning in access privilege provision to officers and formal procedures for when accessing information outside one's given status. Once data is routed over more than a single network (which is often the case when travelling on the Internet), there would be a greater chance of information being hijacked or intercepted. Although the routing and transmission protocols will be defined by the government appointed agencies who supply and maintain the required technology, however, individuals (cardholders) usually have no knowledge of how the information is accessed, how it is being delivered, and which routes it takes to travel through networks. In reality Internet and network traffic and data management are far more complicated than we have discussed above, and to reach the desired level of service there will be a huge pressure being placed on technology chosen. It would require exponential computing capabilities to provide for efficiency, accuracy, consistency, and security for the system.

5.2 Electoral Voting and Civil Registration

5.2.1 Type of Data and Sensitivity

An ideal way to utilise a national ID card is to apply it in an electronic voting scheme[3]. In this application the national ID card is issued to one country's legitimate residents therefore also granting their rights for voting. One practical way to apply ID card here is for the cardholder to present his/her card at a voting station and the voter's identity can verified. To authenticate whether an individual has the right to vote, this application needs to acquire the following information from cardholders: Name, Resident Status, Nationality, Age. Note that other information such as Sex, Employment Status, Criminal Records and VISA records are not considered as necessary information here because the main goal here is to determine an individual's right to vote. Therefore nationality, age, and residency status are usually the information needed to form the basis to whether such person has the right to cast a vote on a national or local election. We can then clarify their sensitivity as: Highly Classified - None; Average Confidential - None; Low

[3]generally we refer electronic voting to as an establishment in which individuals are able to cast votes to elections or polls remotely, through compatible devices, and using agreed protocols

Confidential - Name, Nationality, Resident Status, Age. Moreover, if a country had given every citizen a citizen ”ID” number, then this information should be included as when during the check, the system would be able to relate the number to a particular person’s information stored in the backend system.

5.2.2 Practical Deployment and Check Procedures

There are three platforms on which an electronic voting system can be deployed [3], two of which can be network-based:

- Online Poll Website Voting - this can be a website specifically designed for voter to cast votes in a controlled environment, for example, internal company election. There will be one centralised register and tabulation maybe centralised. Only internally registered users may cast votes. Users log into system, verified by server, cast their votes, server acknowledge transaction, user log off system.
- Remote Internet Voting - context will be much wider and can be used for national elections. Residences of a country who are eligible to vote may vote using terminals at home, work, or other mobile devices such as mobile phones and PDAs. Votes cast online using computers will be done in a similar way as online website voting. Users using mobile devices will need to authenticate themselves to the device as well as the server that runs the voting system.
- Kiosk Voting - polling stations can be setup temporarily (manned or unmanned) and access to voting premise must be restricted to voters who have access rights. In a manned station individuals present ID card to gain access to premise, insert card into terminal, card verifies cardholder identity and user identifies himself to server, casts vote, transaction recorded, card ejects. In an unmanned premise, user insert card into entry system to gain access to voting terminal.

5.2.3 Example of Setup for Remote Voting System

Basic setup for an electronic voting system should include the following steps:

1. Voter Authentication - this step involves checking procedures on voter’s identification and his/her eligibility to cast vote.

2. Distribution of Client Application - once the voter's identification has been confirmed, the specifically designed client application can be distributed through he following channels: online download, signed codes, or CD-ROM distribution.

3. Security Setup for Client Terminals - security requirements and setup configurations should be made known to clients to ensure confidentiality, integrity, and efficiency of application and transmission secrecy.

4. Distribution of Election Data - this involves distribution materials such as candidate information, voting period, procedures and so on.

5. Security Setup for Server Terminal - security features of server terminal must also be implemented.

We may simplify these steps as: 1. Setup Entities 2. Voter Registration 3. Distribute Secret Credentials 4. Authenticate Voters 5. Vote Casting 6. Tallying 7. Confirmation Transaction and Result.

5.2.4 Problems and Requirements for Voting Systems

One important aspect in voting scheme is anonymity. Voters participating in a voting scheme should be provided the ability and rights to remain anonymous. Such element is essential in order to preserve user privacy. However, on the other hand, there must be some solution for the authority to be able to ask individuals to vouch for non-repudiation. These two aspects will require a protocol that provides both non-repudiation and anonymity.

The fundamental requirements for a voting system (be it conventional or electronic) include system security and user privacy. This means election process and results must be verifiably correct and individual votes must remain secret. To extend the requirement criteria we may also include the following aspects: 1. Votes can only be cast by registered voters. 2. Each voter may only vote once in a single given election. 3. Privacy of Individual voter must be confirmed. 4. Election result must be verifiable. 5. The system should be robust. 6.Interaction between voters should not be allowed. 7. Votes must not be duplicated. 8. Means must be provided to invalidate votes cast outside the specified time period (freshness checking). Therefore we can say that such system must incorporate means to provide for authentication (to verify the legitimate voter), non-repudiation(non-denial of delivery/receipt of votes), data integrity(modification-free assurance), and anonymity (user privacy).

5.3 Immigration Management

5.3.1 Type of Data and Sensitivity

Traditionally immigration management[4] relied heavily on a precarious structure of letters, certificates, and paper-based documents. These documents attest to an individual's identification, which might include the following information as well: nationality, age, ethnic origin, residency status etc. If the card application is used for immigration control, that means the cards would be mainly issued to those who travel into a specific country. Similar to the data required under the use of card for travel document, a card scheme used for immigration control would require the following basic information about a person to carry out an ID check: Name, Sex, Legal Nationality, Address, Resident Status and VISA Records. Other information that may be added on to the database later may include Employment Status and Criminal Records. The most important pieces of information here include an individual's legal nationality and residency status. This is because an immigration control ID card would generally be used to check whether a person has the right to claim public benefits available to legal citizens, hence to reduce the use of false ID to wrongly claim social benefits. We can categorise them as: Highly Classified - Criminal Records. Average Confidential - VISA Records, Employment Records. Low Confidential - Name, Sex, Nationality, Resident Status, Age.

5.3.2 General Problems

The most obvious problem one would be facing with paper-based immigration identification documents is forgery. Especially in a country where civil documents are issued by large number of government agencies, and the lack of uniformity and standards will result in widespread of forgery abuse. The hidden agenda here is that the security risk from use of falsified documents on other identification applications that depend on individual's identification check. By presenting a falsified immigration document one can gain access to various public services that are not supposed to be made available to them. To overcome such problem an ID card scheme intended to serve to control immigration needs to have security features that are hard to forge, and can be authenticated in ways that forged cards will be recognised instantly. However, there is a greater concern over the success of such scheme and it depends on one of two processes: a vastly increased level of constant checking of the entire population; or checking procedures against target minorities. Either way it requires careful planning.

[4]we refer immigration management to as methods for providing solutions for custom control to reduce risk of forged and counterfeited ID documents at national borders

5.3.3 Practical Deployment

The UK Government has recently issued smart chip ID cards for foreign nationals seeking for asylum. The card has an integrated chip which stores and holder's fingerprints, asylum status, a photograph, and details on their age and nationality. There has already been a database that contains asylum seekers' fingerprints, and to store such information on an ID card could provide an easier way to effectively identify individuals. There are social benefits available to asylum seekers but in order to prevent them from claiming more than what they are entitled to, effective identification check on benefit claimant is a crucial point. In this scheme we can identify the main entities including central data register, cardholder, card user (authorities who use the card to verify a person's identification), card reader, and technology supplier. During an ID verification process, a card is inserted into a reader, the cardholder verifies himself to the card, the card interacts with terminal and retrieve information from central database. The central database may be linked with other local government databases if further checks are to be carried out.

6 Technology Evaluation

After we have seen discussions on the application scenarios and requirements of a identification card scheme, we would then need to evaluate the available technologies and attempt to define a reasonable solution for a secure national identification card scheme. Listed below are few points that we need to discuss before designing and choosing a suitable solution:

- What types of information need to be stored on the ID card? This varies according to what the card will be used for.
- What is the potential future use of the scheme and what is the upgradability of that technology? A key requirement for any identification system is the potential ability for the system to be upgraded without needing major changes in the scheme infrastructure. Upgradability is crucial since changes in infrastructure might change system functionality and require modification in user information. For example, if a security scheme is compromised there would be modifications to system operation but there should not be a need to replace the individual cards.
- Which type of technology has the best standards available? A national ID card scheme would be used by large numbers of government agencies and

business organisations that use different and proprietary technologies. This diversity of use of technology would make it hard to detect counterfeiting as well as limit the use and expandability of the system. An ideal system would define an open architecture for cards and interactive devices, using a common specification standard. Card vendors should also comply with standardised security specifications of card and security.

- How will the card be used and what is the required level of transaction speed and confidentiality? There are numbers of ways to read information from a card including: swipe, scan, sense, and insert. Transaction volume and desired speed of transaction depend on the application of the card.

- What level of security is desired to maintain the required security profile of information? The main reason to implement a card-based identification system is to solve the problem of forgery from paper document-based identification systems. Therefore ID cards must be secure. A secure identification card must be protected by security features so it s difficult to counterfeit, and be able to invalidate itself when being tampered with. It must also have security functions to prevent unlawfully access to information stored on the card and on the backend system.

7 Conclusion

We have briefly identified the main security requirements for applications of a national ID card system. We have also discussed available technologies and evaluation aspects they must comply with. It will be difficult to choose one single technology that has the functionality and capability to meet all the security requirements that we have defined. However, it is not impossible to implement a solution with a combination of technologies. For example, depending on the application requirements, an ID card can be a combination of magnetic stripe, bar code, photo ID, and smart chip, while in some cases maybe a simple magnetic stripe card would be sufficient enough to meet the requirements. However, given the complexity of such system and the related issues it raises (such as privacy issues and technology reliability etc), deeper analysis is still needed.

References

[1] Secure personal identification systems: Policy, process and technology choices for privacy-sensitive solution. Available online at

www.smartcardalliance.org, Feb 2002.

[2] Mike Henry. *Smart Card Security and Applications*. Artech House, Inc., Norwood, MA, 1997.

[3] Berry Schoenmakers. Electronic voting. TU Eindhoven, The Netherlands, January 2003. TU Eindhoven. Conference Notes: Can We Trust Networks? Trends in Network infrastructure and Application Security.